ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА МГУ.012.3
ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ ДОКТОРА НАУК

Решение диссертационного совета от «27» сентября 2023 г., протокол №5,
о присуждении Таранникову Юрию Валерьевичу
ученой степени доктора физико-математических наук

Диссертация **«Конструкции и свойства корреляционно-иммунных и платовидных булевых функций»** по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки) принята к защите диссертационным советом 21 июня 2023 г., протокол № 3.

Соискатель **Таранников Юрий Валерьевич** 1967 года рождения, **в 1991 году** окончил ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», механико-математический факультет, и получил квалификацию «математик» по специальности «математика» (диплом ФБ 217604).

В 1994 **году соискатель защитил диссертацию на соискание ученой степени кандидата физико-математических наук на тему «**Множества l-уравновешенных булевых наборов и функций**»** в совете Д 053.05.05 при ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» по специальности 01.01.09 – дискретная математика и математическая кибернетика (диплом КТ003450).

Соискатель работает на кафедре дискретной математики механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» с 1994 года по настоящее время. С 1994 года в должности младшего научного сотрудника, затем старшего преподавателя, а с 1998 года – доцента этой кафедры.

Диссертация выполнена в ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», механико-математический факультет на кафедре дискретной математики.

Официальные оппоненты:

Алексеев Валерий Борисович, доктор физико-математических наук, профессор, ФГБОУ ВО “Московский государственный университет имени М.В. Ломоносова”, факультет Вычислительной математики и кибернетики, кафедра математической кибернетики, профессор;

Кротов Денис Станиславович, доктор физико-математических наук, профессор РАН, главный научный сотрудник лаборатории алгебраической комбинаторики ФГБУН «Институт математики им. С. Л. Соболева Сибирского отделения Российской академии наук»;

Черемушкин Александр Васильевич, доктор физико-математических наук, профессор, действительный член Академии криптографии РФ, ведущий научный сотрудник лаборатории математических проблем теоретической криптографии Федерального государственного казенного научного учреждения «Академия криптографии Российской Федерации»

дали **положительные отзывы** на диссертацию.

Соискатель имеет 82 опубликованные работы, в том числе по теме диссертации 62 работы, из которых 18 опубликованы в изданиях, индексируемых в Web of Science, Scopus, RSCI, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6 –

Методы и системы защиты информации, информационная безопасность (физико-математические науки).

Публикации в рецензируемых научных изданиях, индексируемых в базах данных Web of Science (WoS), Scopus, RSCI:

1. Тарапников Ю.В. О числе единичных значений l-уравновешенных булевых функций. *Дискретный анализ и исследование операций*. 1995. Т. 2, №1, с.80-81 (РИНЦ 0.535).

2. Тарапников Ю.В. О некоторых оценках для веса l-уравновешенных булевых функций. *Дискретный анализ и исследование операций*. 1995. Т. 2, №4. с. 80-96 (РИНЦ 0.535).

[Перевод на английский язык: Tarannikov Yu.V. On certain bounds for the weight of l-balanced Boolean functions. *Mathematics and Its Applications*, V.391, Korshunov A.D. (ed.), Operation Research and Discrete Analysis, 1997, 285-299.]

3. Тарапников Ю. В. О классе булевых функций, равномерно распределенных по шарам со степенью 1. *Вестник Московского университета, Серия 1, Математика, Механика*, 1997, N 5, с. 17-21 (РИНЦ 0.472).

[Перевод на английский язык: Tarannikov Yu. A class of Boolean functions homogeneously distributed over balls with degree 1. *Moscow University Mathematics Bulletin*. – 1997. – Vol. 52, № 5. – pp.18-22 (SJR 0.417).]

4. Carlet C., Tarannikov Yu. Covering sequences of Boolean functions and their cryptographic significance. *Designs, Codes and Cryptography*, V. 25, 2002, pp. 263-279 (SJR 1.122) // Ю.В. Тарапников получил результаты разделов 5 и 6.

5. Fedorova M., Tarannikov Yu. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices. *Progress in Cryptology* – Indocrypt 2001, Chennai, India, December 16-20, 2001, Proceedings, Lecture Notes in Computer Science, V. 2247, pp. 254-266, Springer-Verlag, 2001 (SJR 0.407) // Ю.В. Тарапников получил результаты разделов 5, 6 и 7.

6. Tarannikov Yu. On the structure and numbers of higher order correlation-immune functions. *Proceedings of 2000 IEEE International Symposium on Information Theory ISIT2000*, Sorrento, Italy, June 25-30, 2000, p. 185 (SJR 0.872).

7. Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity. *Proceedings of Indocrypt 2000*, Lecture Notes in Computer Science, V. 1977, pp. 19-30, Springer-Verlag, 2000 (SJR 0.407).

8. Tarannikov Yu., Kirienko D. Spectral analysis of high order correlation immune functions. *Proceedings of 2001 IEEE International Symposium on Information Theory ISIT2001*, Washington, DC, USA, June 2001, p. 69 (SJR 0.872) // Ю.В. Тарапников доказал теоремы 1, 2, 3 и частично 4.

9. Tarannikov Yu., Korolev P., Botev A. Autocorrelation coefficients and correlation immunity of Boolean functions. *Proceedings of Asiacrypt 2001*, Gold Coast, Australia, December 9-13, 2001, Lecture Notes in Computer Science, V. 2248, pp. 460-479, Springer-Verlag, 2001 (SJR 0.407) // Ю.В. Тарапников получил результаты разделов 3, 4 и 7.

10. Tarannikov Y. New constructions of resilient Boolean functions with maximal nonlinearity. *Fast Software Encryption*, 8th International Workshop, FSE 2001, Yokohama, Japan, April 2-4, 2001. Revised Papers. Lecture Notes in Computer Science. Vol. 2355, pp. 66-77, Springer-Verlag, 2002 (SJR 0.407).

11. Fedorova M., Tarannikov Yu. On impossibility of uniform distribution of codewords over

spheres in some cases. *Proceedings of 2002 IEEE International Symposium on Information Theory ISIT2002*, Lausanne, Switzerland, June 30 — July 05, 2002. — 2002. — p. 344 (SJR 0.872) // Ю.В. Тарannиков предложил постановку задачи, методику исследований и рассмотрел случай l=1.

12. Тарannиков Ю. В. О значениях аффинного ранга носителя спектра платовидной функции. *Дискретная математика*. — 2006. — Т. 18, № 3. — с. 120-137 (РИНЦ 0.624).

[Перевод на английский язык: Tarannikov Yu. V. On values of the affine rank of the support of spectrum of a plateaued function. *Discrete Mathematics and Applications*. — 2006. — Vol. 16, № 4. — pp. 401-421 (SJR 0.226).]

13. Tarannikov Yu. Generalized proper matrices and constructing of m-resilient Boolean functions with maximal nonlinearity for expanded range of parameters. *Siberian electronic mathematical reports*. — 2014. — Vol. 11. — pp. 229-245 (SJR 0.516).

14. Тарannиков Ю. В. О рангах подмножеств пространства двоичных векторов, допускающих встраивание системы Штейнера S(2,4,v). *Прикладная дискретная математика*. — 2014. — № 1 (23). — с. 73-76 (РИНЦ 0.368, SJR 0.214).

15. Sauskan A.V., Tarannikov Yu.V. On packings of (n, k)-products. *Siberian electronic mathematical reports*. — 2016. — Vol. 13. — pp. 888-896 (SJR 0.516) // А.В. Саускан выдвинул идею рекурсивной конструкции в доказательстве теоремы 2; Ю.В. Тарannиков сделал остальное.

16. Khalyavin A. V., Lobanov M. S., Tarannikov Yu. V. On plateaued Boolean functions with the same spectrum support. *Siberian electronic mathematical reports*. — 2016. — Vol. 13. — pp. 1346-1368 (SJR 0.516) // Ю.В. Тарannиков получил результаты раздела 3, написал обзор в разделе 1, а также принял участие в доказательстве результатов раздела 2.

17. Баксова И. П., Тарannиков Ю. В. Оценки числа разбиений пространства $\mathbf{F}_2^m$ на аффинные подпространства размерности k. *Вестник Московского университета. Серия 1: Математика. Механика.* — 2022. — № 3. — с. 21-25 (РИНЦ 0.472) // Ю.В. Тарannиков предложил постановку задачи и методику исследований.

[Перевод на английский язык: Baksova I. P., Tarannikov Yu. V. The bounds on the number of partitions of the space $\mathbf{F}_2^m$ into k-dimensional affine subspaces. *Moscow University Mathematics Bulletin*. — 2022. — Vol. 77, № 3. — pp. 131-135 (SJR 0.417).]

18. Тарannиков Ю. В. О существовании разбиений, примитивных по Агиевичу. *Дискретный анализ и исследование операций*. — 2022. — Т. 29, № 4. — с. 104-123 (РИНЦ 0.535).

[Перевод на английский язык: Tarannikov Y. V. On the existence of Agievich-primitive partitions. *Journal of Applied and Industrial Mathematics*. — 2022. — Vol. 16, № 4 — pp. 809-820 (SJR 0.391).]

Публикации в рецензируемых научных изданиях, входящих в перечень ВАК Минобрнауки России:

19. Тарannиков Ю. В. О критериях бесконечности инвариантных классов дискретных функций, *Математические вопросы кибернетики*, Вып. 9, М., Физматлит, 2000, с. 59-78.

20. Тарannиков Ю. В. О корреляционно-иммунных и устойчивых булевых функциях, *Математические вопросы кибернетики* / Под ред. О. Б. Лупанов. — Т. 11 из Математические вопросы кибернетики. — М.: Физматлит, 2002. — С. 91-148.

На автореферат диссертации поступили 3 **дополнительных отзыва, все положительные**.

Выбор официальных оппонентов обоснован их высокой профессиональной квалификацией, наличием научных публикаций по направлениям, тесно связанным с темой диссертации автора, а также их соответствием критериям, установленным в Положении о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова.

Диссертационный совет отмечает, что представленная диссертация на соискание ученой степени доктора физико-математических наук **является научно-квалификационной работой**, в которой на основании выполненных автором исследований **достигнуты существенные результаты в решении важной в теоретическом плане и практическом отношении проблемы** обеспечения стойкости систем защиты информации против корреляционных криптографических атак в математических моделях информационной безопасности.

Диссертация представляет собой **самостоятельное законченное исследование, обладающее внутренним единством**. Положения, выносимые на защиту, содержат новые научные результаты, которые свидетельствуют **о личном вкладе автора** в науку:

1. Верхняя оценка нелинейности $2^{n-1}-2^{m+1}$ для m-устойчивых функций от n переменных, которая может достигаться только на функциях, достигающих равенства в неравенстве Зигенталера.

2. Методы построения m-устойчивых функций от n переменных с максимально возможной нелинейностью $2^{n-1}-2^{m+1}$, в частности, с использованием введенных автором подходящих и обобщенных подходящих матриц.

3. Конструкции m-устойчивых функций от n переменных с нелинейностью $2^{n-1}-2^{m+1}$ при всех па́рах (m,n), удовлетворяющих неравенству $0{,}6n-1\le m\le n-2$, а асимптотически – при выполнении условия $0{,}5789\ldots(1+o(1))\le m/n$.

4. Нижняя оценка глобальной автокорреляционной характеристики m-устойчивой функции от n переменных.

5. Вид формул для числа корреляционно-иммунных и устойчивых порядка $m=n-k$ булевых функций от n переменных, являющихся полиномом степени $p(k)$; оценки для величины $p(k)$.

6. Конструкции платовидных функций с носителем спектра мощности 4^h и аффинным рангом $\mathbf{k}$ для любого натурального $\mathbf{k}$, удовлетворяющего неравенствам $2h\le \mathbf{k}\le 2^{h+1}-2$.

7. Нижние и верхние оценки для величины $N_q(m)$, где $N=N_q(m)$ – наименьшее натуральное число, такое что при $n>N$ не существует A-примитивных разбиений $\mathbf{F}_q{}^n$ на q^m аффинных подпространств размерности $n-m$, а q – степень простого числа; точное значение $N_q(2)=q+1$.

8. Близость при больших n плотности *l*-уравновешенных функций к одному из следующих пяти чисел: 0, $1/3$, $1/2$, $2/3$ или 1.

9. Критерий, позволяющий по системе запрещенных подфункций, задающих инвариантный класс, определить, содержит ли этот класс бесконечное число существенно разных функций, и сводящий рассматриваемую задачу для функций к соответствующей задаче для множеств слов.

Результаты диссертации базируются на известных теоретических положениях арифметики, элементарной, линейной и высшей алгебры, теории функций, перечислительной и словарной комбинаторики, теории комбинаторных дизайнов, теории сложности вычислений, **являются четко сформулированными**, а их **достоверность обеспечивается** строгими математическими доказательствами. **Все результаты диссертации являются новыми**. Результаты других авторов, упомянутые в диссертации, отмечены соответствующими ссылками. **Результаты диссертации прошли апробацию** на многочисленных международных и всероссийских конференциях, симпозиумах и научно-исследовательских семинарах. Основные результаты опубликованы в научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Сформулированные в диссертации положения доказаны автором самостоятельно, **они теоретически и практически значимы, являются существенным продвижением в решении важной в теоретическом плане и практическом отношении проблемы** обеспечения стойкости систем защиты информации против корреляционных криптографических атак в математических моделях информационной безопасности. Результаты могут найти применение в теории защиты информации, теории синтеза схем, теории кодирования, математической кибернетике, дискретной математике. Разработанные в ходе диссертационных исследований методы, построенные функции и смежные объекты, установленные свойства, в частности, разработанные эффективные схемные и программные методы реализации m-устойчивых функций от n переменных, могут применяться в криптографических примитивах и системах защиты информации, в частности, в поточных шифрах. Возможно применение метода, включающего обобщенные подходящие матрицы, для построения систем функций, а также в блочных шифрах. Результаты по корреляционно-иммунным функциям могут быть задействованы при разработке криптографических масок.

На заседании 27 сентября 2023 года диссертационный совет принял решение присудить Таранникову Ю.В. ученую степень доктора физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 21 человека, из них 5 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали:

за - 21, против - нет, недействительных бюллетеней - нет.

Заместитель председателя
диссертационного совета МГУ.012.3,
доктор физико-математических наук, профессор В.А. Васенин

Ученый секретарь
диссертационного совета МГУ.012.3,
кандидат физико-математических наук А.В. Галатенко

«27» сентября 2023 г.